Schedule 16 (Security) (Short Form)

1. **Supplier obligations**

Core requirements

1.1 The Supplier must comply with the core requirements set out in Paragraphs 3 to 9.

1.2 Where the Buyer has selected an option in the table below, the Supplier must comply with the requirements relating to that option set out in the relevant Paragraph:

Certifications (see Paragraph 4) [to be completed post contract award – please refer to Appendix 1 - Functional and Non-functional Specification of Requirements to understand required Certifications]		
The Supplier must have the following Certifications (or equivalent):	ISO/IEC 27001:2022 by a UKAS-recognised Certification Body	☐
	Cyber Essentials Plus	☐
	Cyber Essentials	☐
	No certification required	☐
Subcontractors that Handle Buyer Data must have the following Certifications (or equivalent):	ISO/IEC 27001:2022 by a UKAS-recognised Certification Body	☐
	Cyber Essentials Plus	☐
	Cyber Essentials	☐
	No certification required	☐
Locations (see Paragraph 5) [to be completed post contract award – please refer to Appendix 1 - Functional and Non-functional Specification of Requirements to understand required Locations please refer to Appendix 1 - Functional and Non-functional Specification of Requirements to understand required Certifications]]		
The Supplier and Subcontractors may store, access or Handle Buyer Data in:	the United Kingdom only	☐
	a location permitted by and in accordance with any regulations for the time being in force made under section 17A of the Data Protection Act 2018 (adequacy decisions by the Secretary of State).	☒
	anywhere in the world not prohibited by the Buyer	☐

Staff vetting (see Paragraph 6)	
The Buyer requires a staff vetting procedure other than BPSS	☐
Where an alternative staff vetting procedure is required, that procedure is:	

Optional requirements

1.3 Where the Buyer has selected an option in the table below, the Supplier must comply with the requirements of the corresponding Paragraph. Where the Buyer has not selected an option, the corresponding requirement does not apply.

Security Management Plan (see Paragraph 10)	
The Supplier must provide the Buyer with a Security Management Plan detailing how the requirements for the options selected in this table have been met.	☒
Buyer Security Policies (see Paragraph 11)	
The Buyer requires the Supplier to comply with the following policies relating to security management as set out in Appendix 1 – Functional and Non-functional Requirements.	☒
Security testing (see Paragraph 12)	
The Supplier must undertake security testing at least once every Contract Year and remediate any vulnerabilities, where it is technically feasible to do so	☒
Cloud Security Principles (see Paragraph 13)	
The Supplier must assess the Supplier System against the Cloud Security Principles	☒
Record keeping (see Paragraph 14)	
The Supplier must keep records relating to Subcontractors, Sites, Third-party Tools and third parties	☒
Encryption (see Paragraph 15)	
The Supplier must encrypt Buyer Data while at rest or in transit	☒
Protective Monitoring System (see Paragraph 16)	
The Supplier must implement an effective Protective Monitoring System	☒
Patching (see Paragraph 17)	

The Supplier must patch vulnerabilities in the Supplier System promptly	☒
Malware protection (see Paragraph 18)	
The Supplier must use appropriate Anti-virus Software	☒
End-user Devices (see Paragraph 19)	
The Supplier must manage End-user Devices appropriately	☒
Vulnerability scanning (see Paragraph 20)	
The Supplier must scan the Supplier System monthly for unpatched vulnerabilities	☒
Access control (see Paragraph 21)	
The Supplier must implement effective access control measures for those accessing Buyer Data and for Privileged Users	☒
Remote Working (see Paragraph 22)	
The Supplier may allow Supplier Staff to undertake Remote Working once an approved Remote Working Policy is in place	☒
Backup and recovery of Buyer Data (see Paragraph 23)	
The Supplier must have in place systems for the backup and recovery of Buyer Data	☒
Return and deletion of Buyer Data (see Paragraph 24)	
The Supplier must return or delete Buyer Data when requested by the Buyer	☒
Physical security (see Paragraph 25)	
The Supplier must store Buyer Data in physically secure locations	☒
Security breaches (see Paragraph 26)	
The Supplier must report any Breach of Security to the Buyer promptly	☒
Cyber Insurance	
The Supplier must have in place a valid Cyber Insurance policy issued by an accredited body and indicate the type of policy coverage	☒

2. **Definitions**

In this Schedule 16 (*Security*):

"Anti-virus Software" software that:

(a) protects the Supplier System from the possible introduction of Malicious Software;

(b) scans for and identifies possible Malicious Software in the Supplier System;

(c) if Malicious Software is detected in the Supplier System, so far as possible:

(i) prevents the harmful effects of the Malicious Software; and

(ii) removes the Malicious Software from the Supplier System;

"BPSS" the employment controls applied to any individual member of the Supplier Staff that performs any activity relating to the provision or management of the Services, as set out in **"**HMG Baseline Personnel Standard**"**, Version 7.0, June 2024 (https://www.gov.uk/government/publications/government-baseline-personnel-security-standard), as that document is updated from time to time;

"Breach of Security" the occurrence of:

(a) any unauthorised access to or use of the Services, the Sites, the Supplier System and/or the Buyer Data;

(b) the loss (physical or otherwise), corruption and/or unauthorised disclosure of any Buyer Data, including copies of such Buyer Data; and/or

(c) any part of the Supplier System ceasing to be compliant with the required Certifications;

(d) the installation of Malicious Software in the Supplier System:

(e) any loss of operational efficiency or failure to operate to specification as the result of the installation or operation of Malicious Software in the Supplier System; and

(f) includes any attempt to undertake the activities listed in sub-Paragraph (a) where the Supplier has reasonable grounds to suspect that attempt:

(i) was part of a wider effort to access information and communications technology operated by or on behalf of Central Buyer Bodies; or

(ii) was undertaken, or directed by, a state other than the United Kingdom;

"Buyer Security Policies"	those security policies specified by the Buyer in Paragraph 1.3;
"Certifications"	one or more of the following certifications (or equivalent): (a) ISO/IEC 27001:2022 by a UKAS-recognised Certification Body in respect of the Supplier System, or in respect of a wider system of which the Supplier System forms part; and (b) Cyber Essentials Plus; and/or (c) Cyber Essentials;
"CHECK Scheme"	the NCSC's scheme under which approved companies can conduct authorised penetration tests of public sector and critical national infrastructure systems and networks;
"CHECK Service Provider"	a company which, under the CHECK Scheme: (a) has been certified by the NCSC; (b) holds **"**Green Light**"** status; and (c) is authorised to provide the IT Health Check services required by Paragraph 7 (*Security Testing*);
"Cloud Security Principles"	the NCSC's document **"**Implementing the Cloud Security Principles**"** as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles;
"CREST Service Provider"	a company with an information security accreditation of a security operations centre qualification from CREST International;
"Cyber Essentials"	the Cyber Essentials certificate issued under the Cyber Essentials Scheme;
"Cyber Essentials Plus"	the Cyber Essentials Plus certificate issued under the Cyber Essentials Scheme;

"Cyber Essentials Scheme"	the Cyber Essentials scheme operated by the NCSC;
"End-user Device"	any personal computers, laptops, tablets, terminals, smartphones or other portable electronic device provided by the Supplier or a Subcontractor and used in the provision of the Services;
"Expected Behaviours"	the expected behaviours set out and updated from time to time in the Buyer Security Classification Policy, currently found at paragraphs 12 to 16 and in the table below paragraph 16 of https://www.gov.uk/government/publications/government-security-classifications/guidance-11-working-at-official-html;
"Government Security Classification Policy"	the policy, as updated from time to time, establishing an administrative system to protect information assets appropriately against prevalent threats, including classification tiers, protective security controls and baseline behaviours, the current version of which is found at https://www.gov.uk/government/publications/government-security-classifications;
"IT Health Check"	the security testing of the Supplier System;
"NCSC"	the National Cyber Security Centre, or any successor body performing the functions of the National Cyber Security Centre;
"NCSC Device Guidance"	the NCSC's document **"**Device Security Guidance**"**, as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/device-security-guidance;
"Privileged User"	a user with system administration access to the Supplier System, or substantially similar access privileges;
"Prohibition Notice"	the meaning given to that term by Paragraph 5.4.
"Protective Monitoring System"	has the meaning given to that term by Paragraph 16.1;
"Relevant Conviction"	any previous or pending prosecution, conviction or caution (excluding any spent conviction under the Rehabilitation of Offenders Act 1974) relating to offences involving dishonesty, terrorism, immigration, firearms, fraud, forgery, tax evasion, offences against people (including sexual offences) or any other offences relevant to Services as the Buyer may specify;
"Remote Location"	the relevant Supplier Staff's permanent home address authorised by the Supplier or Sub-contractor (as applicable) for

	Remote Working OR a location other than a Supplier's or a Sub-contractor's Site;
"Remote Working"	the provision or management of the Services by Supplier Staff from a location other than a Supplier's or a Sub-contractor's Site;
"Remote Working Policy"	the policy prepared and approved under Paragraph 22 under which Supplier Staff are permitted to undertake Remote Working;
"Security Controls"	the security controls set out and updated from time to time in the Government Security Classification Policy, currently found at Paragraph 12 of https://www.gov.uk/government/publications/government-security-classifications/guidance-15-considerations-for-security-advisors-html;
"Sub-contractor"	for the purposes of this Schedule 16 (*Security*) only, any individual or entity that: (a) forms part of the supply chain of the Supplier; and (b) has access to, hosts, or performs any operation on or in respect of the Supplier Information Management System, the Development Environment, the Code and the Buyer Data, and this definition shall apply to this Schedule 16 in place of the definition of Sub-Contractor in Schedule 1 *(Definitions)*;
"Supplier Staff"	for the purposes of this Schedule 16 (*Security*) only, any individual engaged, directly or indirectly, or employed by the Supplier or any Sub-contractor (as that term is defined for the purposes of this Schedule 16 (*Security*) in the management or performance of the Supplier's obligations under this Contract, and this definition shall apply to this Schedule 16 (*Security*) in place of the definition of Supplier Staff in Schedule 1 (*Definitions*);
"Third-party Tool"	any software used by the Supplier by which the Buyer Data is accessed, analysed or modified, or some form of operation is performed on it; and
UKAS-recognised Certification Body	(a) an organisation accredited by UKAS to provide certification of ISO/IEC27001:2013 and/or ISO/IEC27001:2022; or (b) an organisation accredited to provide certification of ISO/IEC27001:2013 and/or ISO/IEC27001:2022 by a body with the equivalent functions as UKAS in a state with which the UK has a mutual recognition agreement

recognising the technical equivalence of accredited conformity assessment.

Part One: Core Requirements

3. **Handling Buyer Data**

3.1 The Supplier acknowledges that it:

3.1.1 must only Handle Buyer Data that is classified as OFFICIAL; and

3.1.2 must not Handle Buyer Data that is classified as SECRET of TOP SECRET.

3.2 The Supplier must:

3.2.1 not alter the classification of any Buyer Data

3.2.2 if it becomes aware that it has Handled any Buyer Data classified as SECRET or TOP SECRET the Supplier must:

(i) immediately inform the Buyer; and

(ii) follow any instructions from the Buyer concerning that Buyer Data.

3.3 The Supplier must, and must ensure that Sub-contractors and Supplier Staff, when Handling Buyer Data, comply with:

3.3.1 the Expected Behaviours; and

3.3.2 the Security Controls.

4. **Certification Requirements**

4.1 Where the Buyer has not specified Certifications under Paragraph 1, the Supplier must ensure that it and any Subcontractors that Handle Buyer Data are certified as compliant with Cyber Essentials (or equivalent).

4.2 Where the Buyer has specified Certifications under Paragraph 1, the Supplier must ensure that both:

4.2.1 it; and

4.2.2 any Subcontractor that Handles Buyer Data,

are certified as compliant with the Certifications specified by the Buyer in Paragraph 1 (or equivalent certifications).

4.3 The Supplier must ensure that the specified Certifications (or their equivalent) are in place for it and any relevant Subcontractor:

4.3.1 before the Supplier or any Subcontractor Handles Buyer Data; and

4.3.2 throughout the Contract Period.

5. **Location**

5.1 Where the Buyer has not specified any locations or territories in Paragraph 1, the Supplier must not, and ensure that Subcontractors do not store, access or Handle Buyer Data outside:

5.1.1 the United Kingdom; or

5.1.2 a location permitted by and in accordance with any regulations for the time being in force made under section 17A of the Data Protection Act 2018 (adequacy decisions by the Secretary of State).

5.2 Where the Buyer has specified locations or territories in Paragraph 1, the Supplier must, and ensure that all Subcontractors, at all times store, access or Handle Buyer Data only in or from the geographic areas specified by the Buyer.

5.3 The Supplier must, and must ensure that its Subcontractors store, access or Handle Buyer Data in a facility operated by an entity where:

5.3.1 the entity has entered into a binding agreement with the Supplier or Subcontractor (as applicable);

5.3.2 that binding agreement includes obligations on the entity in relation to security management at least as onerous as those relating to Sub-contractors in this Schedule 16 (*Security*);

5.3.3 the Supplier or Subcontractor has taken reasonable steps to assure itself that:

(i) the entity complies with the binding agreement; and

(ii) the Subcontractor's system has in place appropriate technical and organisational measures to ensure that the Sub-contractor will store, access, manage and/or Handle the Buyer Data as required by this Schedule 16 (*Security*); and

5.3.4 the Buyer has not given the Supplier a Prohibition Notice under Paragraph 5.4.

5.4 The Buyer may by notice in writing at any time give notice to the Supplier that it and its Subcontractors must not undertake or permit to be undertaken the storage, accessing or Handling of Buyer Data in one or more countries or territories (a **"Prohibition Notice"**).

5.5 Where the Supplier must and must ensure Subcontractors comply with the requirements of a Prohibition Notice within 40 Working Days of the date of the notice.

6. **Staff vetting**

6.1 The Supplier must not allow, and must ensure that Subcontractors do not allow, Supplier Staff, to access or Handle Buyer Data, if that person has not undergone:

6.1.1 the checks required for the BPSS to verify:

(i) the individual's identity;

(ii) where that individual will work in the United Kingdom, the individual's nationality and immigration status so as to demonstrate that they have a right to work in the United Kingdom; and

(iii) the individual's previous employment history;

(iv) that the individual has no Relevant Convictions; and

(v) national security vetting clearance to the level specified by the Buyer for such individuals or such roles as the Buyer may specify; or

(vi) such other checks for the Supplier Staff as the Buyer may specify.

6.2 Where the Supplier considers it cannot ensure that a Sub-contractors will undertake the relevant security checks on any Sub-contractor Staff, it must:

6.2.1 as soon as practicable, and in any event within 20 Working Days of becoming aware of the issue, notify the Buyer;

6.2.2 provide such information relating to the Sub-contractor, its vetting processes and the roles the affected Sub-contractor Staff will perform as the Buyer reasonably requires; and

6.2.3 comply, at the Supplier's cost, with all directions the Buyer may provide concerning the vetting of the affected Sub-contractor Staff and the management of the Sub-contractor.

7. **Supplier assurance letter**

7.1 The Supplier must, no later than the last day of each Contract Year, provide to the Buyer a letter from its chief technology officer (or equivalent officer) confirming that, having made due and careful enquiry:

7.1.1 the Supplier has in the previous year carried out all tests and has in place all procedures required in relation to security matters required by this Contract;

7.1.2 it has fully complied with all requirements of this Schedule 16 (*Security*);

7.1.3 all Subcontractors have complied with the requirements of this Schedule 16 (*Security*) with which the Supplier is required to ensure they comply; and

7.1.4 the Supplier considers that its security and risk mitigation procedures remain effective.

8. **Assurance**

8.1 The Supplier must provide such information and documents as the Buyer may request in order to demonstrate the Supplier's and any Subcontractors' compliance with this Schedule 16 (*Security*).

8.2 The Supplier must provide that information and those documents:

8.2.1 at no cost to the Buyer;

8.2.2 within 10 Working Days of a request by the Buyer;

8.2.3 except in the case of original document, in the format and with the content and information required by the Buyer; and

8.2.4 in the case of original document, as a full, unedited and unredacted copy.

9. **Use of Subcontractors and third parties**

9.1 The Supplier must ensure that Subcontractors and any other third parties that store, have access to or Handle Buyer Data comply with the requirements of this Schedule 16 (*Security*).

Part Two: Additional Requirements

10. Security Management Plan

10.1 This Paragraph 10 applies only where the Buyer has selected this option in Paragraph 1.3.

Preparation of Security Management Plan

10.2 The Supplier shall document in the Security Management Plan how the Supplier and its Sub-contractors shall comply with the requirements set out in this Schedule 16 (*Security*) and the Contract in order to ensure the security of the Supplier solution and the Buyer data.

10.3 The Supplier shall prepare and submit to the Buyer within 20 Working Days of the Effective Date, the Security Management Plan, which must include a description of how all the options selected in this schedule are being met along with evidence of the required certifications for the Supplier and any Subcontractors specified in Paragraph 3.

Approval of Security Management Plan

10.4 The Buyer shall review the Supplier's proposed Security Management Plan as soon as possible and must issue the Supplier with either:

10.4.1 an information security approval statement, which shall confirm that the Supplier may operate the service and process Buyer data; or

10.4.2 a rejection notice, which shall set out the Buyer's reasons for rejecting the Security Management Plan.

10.5 If the Buyer rejects the Supplier's proposed Security Management Plan, the Supplier must prepare a revised Security Management Plan taking the Buyer's reasons into account, which the Supplier must submit to the Buyer for review within 10 Working Days of the date of the rejection, or such other period agreed with the Buyer.

10.6 The process set out in Paragraph 10.5 shall be repeated until such time as the Buyer issues a Risk Management Approval Statement to the Supplier or terminates this Contract.

10.7 The rejection by the Buyer of a second revised Security Management Plan is a material Default of this Contract.

Updating Security Management Plan

10.8 The Supplier shall regularly review and update the Security Management Plan, and provide such to the Buyer, at least once each year and as required by this Paragraph.

Monitoring

10.9 The Supplier shall notify the Buyer within 2 Working Days after becoming aware of:

10.9.1 a significant change to the components or architecture of the Supplier System;

10.9.2 a new risk to the components or architecture of the Supplier System;

10.9.3 a vulnerability to the components or architecture of the Supplier System using an industry standard vulnerability scoring mechanism;

10.9.4 a change in the threat profile;

10.9.5 a significant change to any risk component;

10.9.6 a significant change in the quantity of Personal Data held within the Service;

10.9.7 a proposal to change any of the Sites from which any part of the Services are provided; and/or

10.9.8 an ISO27001 audit report produced in connection with the Certification indicates significant concerns.

10.10 Within 10 Working Days of such notifying the Buyer or such other timescale as may be agreed with the Buyer, the Supplier shall make the necessary changes to the Security Management Plan and submit the updated Security Management Plan to the Buyer for review and approval.

11. Buyer Security Policies

11.1 The Supplier must comply, when it provides the Services and operates and manages the Supplier System, with all Buyer Security Policies identified in the relevant option in Paragraph 1.3.

11.2 If there is an inconsistency between the Buyer Security Policies and the requirement of this Schedule 16 (*Security*), then the requirements of this Schedule will prevail to the extent of that inconsistency.

12. Security testing

12.1 The Supplier must:

12.1.1 before Handling Buyer Data;

12.1.2 at least once during each Contract Year; and

12.1.3 undertake the following activities:

12.1.4 conduct security testing of the Supplier System (an **"IT Health Check"**) in accordance with Paragraph 12.2; and

12.1.5 implement any findings, and remedy any vulnerabilities identified by the IT Health Check in accordance with Paragraph 12.3.

12.2 In arranging an IT Health Check, the Supplier must:

12.2.1 use only a CHECK Service Provider or CREST Service Provider to perform the IT Health Check;

12.2.2 design and plan for the IT Health Check so as to minimise the impact of the IT Health Check on the Supplier System and the delivery of the Services;

12.2.3 ensure that the scope of the IT Health Check encompasses the components of the Supplier System used to access, store, Handle or manage Buyer Data; and

12.2.4 ensure that the IT Health Check provides for effective penetration testing of the Supplier System.

12.3 The Supplier treat any vulnerabilities as follows:

12.3.1 the Supplier must remedy any vulnerabilities classified as high in the IT Health Check report:

(i) if it is technically feasible to do so, within 5 Working Days of becoming aware of the vulnerability and its classification; or

(ii) if it is technically feasible to remedy the vulnerability but not technically feasible to do so as required by Paragraph 12.3.1(i), then as soon as reasonably practicable after becoming aware of the vulnerability and its classification;

12.3.2 the Supplier must remedy any vulnerabilities classified as high in the IT Health Check report:

(i) if it is technically feasible to do so, within 1 month of becoming aware of the vulnerability and its classification; or

(ii) if it is technical feasible to remedy the vulnerability but not technically feasible to do so as required by Paragraph 12.3.2(i), then as soon as reasonably practicable after becoming aware of the vulnerability and its classification;

12.3.3 the Supplier must remedy any vulnerabilities classified as medium in the IT Heath Check report:

(i) if it is technically feasible to do so, within 3 months of becoming aware of the vulnerability and its classification; or

(ii) if it is technical feasible to remedy the vulnerability but not technically feasible to do so as required by Paragraph 12.3.3(i), then as soon as reasonably practicable after becoming aware of the vulnerability and its classification; or

12.3.4 where it is not technically feasible to remedy the vulnerability, the Supplier must implement appropriate technical and organisational measures to mitigate the risk posed by the vulnerability.

13. Cloud Security Principles

13.1 The Supplier must ensure that the Supplier System complies with the Cloud Security Principles.

13.2 The Supplier must assess the Supplier System against the Cloud Security Principles to assure itself that it complies with Paragraph 13.1:

13.2.1 before Handling Buyer Data;

13.2.2 at least once each Contract Year; and

13.2.3 when required by the Buyer.

13.3 Where the Cloud Security Principles provide for various options, the Supplier must document the option it has chosen to implement and its reasons for doing so.

13.4 The Supplier must:

13.4.1 keep records of any assessment that it makes under Paragraph 13.2; and

13.4.2 provide copies of those records to the Buyer within 10 Working Days of any request by the Buyer.

14. Information about Subcontractors, Sites and Third-party Tools

14.1 The Supplier must keep the following records:

14.1.1 for Subcontractors or third parties that store, have access to or Handle Buyer Data:

(i) the Subcontractor or third-party's name:

(A) legal name;

(B) trading name (if any); and

(C) registration details (where the Subcontractor is not an individual), including:

(1) country of registration;

(2) registration number (if applicable); and

(3) registered address;

(ii) the Certifications held by the Subcontractor or third party;

(iii) the Sites used by the Subcontractor or third party;

(iv) the Services provided or activities undertaken by the Subcontractor or third party;

(v) the access the Subcontractor or third party has to the Supplier System;

(vi) the Buyer Data Handled by the Subcontractor or third party; and

(vii) the measures the Subcontractor or third party has in place to comply with the requirements of this Schedule 16 (*Security*);

14.1.2 for Sites from or at which Buyer Data is accessed or Handled:

(i) the location of the Site;

(ii) the operator of the Site, including the operator's:

(A) legal name;

(B) trading name (if any); and

(C) registration details (where the Subcontractor is not an individual);

(iii) the Certifications that apply to the Site;

(iv) the Buyer Data stored at, or Handled from, the site; and

14.1.3 for Third-party Tools:

(i) the name of the Third-party Tool;

(ii) the nature of the activity or operation performed by the Third-Party Tool on the Buyer Data; and

(iii) in respect of the entity providing the Third-Party Tool, its:

(A) full legal name;

(B) trading name (if any)

(C) country of registration;

(D) registration number (if applicable); and

(E) registered address.

14.2 The Supplier must update the records it keeps in accordance with Paragraph 14.1:

14.2.1 at least four times each Contract Year;

14.2.2 whenever a Subcontractor, third party that accesses or Handles Buyer Data, Third-party Tool or Site changes; or

14.2.3 whenever required to go so by the Buyer.

14.3 The Supplier must provide copies of the records it keeps in accordance with Paragraph 14.1 to the Buyer within 10 Working Days of any request by the Buyer.

15. **Encryption**

15.1 The Supplier must, and must ensure that all Subcontractors, encrypt Buyer Data:

15.1.1 when stored at any time when no operation is being performed on it, including when stored on any portable storage media; and

15.1.2 when transmitted.

16. **Protective Monitoring System**

16.1 The Supplier must, and must ensure that Subcontractors, implement an effective system of monitoring and reports, analysing access to and use of the Supplier System and the Buyer Data to:

16.1.1 identify and prevent any potential Breach of Security;

16.1.2 respond effectively and in a timely manner to any Breach of Security that does;

16.1.3 identify and implement changes to the Supplier System to prevent future any Breach of Security; and

16.1.4 help detect and prevent any potential criminal offence relating to fraud, bribery or corruption using the Supplier System,

(the **"Protective Monitoring System"**).

16.2 The Protective Monitoring System must provide for:

16.2.1 event logs and audit records of access to the Supplier System; and

16.2.2 regular reports and alerts to identify:

(i) changing access trends;

(ii) unusual usage patterns; or

(iii) the access of greater than usual volumes of Buyer Data; and

(iv) the detection and prevention of any attack on the Supplier System using common cyber-attack techniques.

17. Patching

17.1 The Supplier must, and must ensure that Subcontractors, treat any public releases of patches for vulnerabilities as follows:

17.1.1 the Supplier must patch any vulnerabilities classified as "critical":

(i) if it is technically feasible to do so, within 5 Working Days of the public release; or

(ii) if it is technical feasible to patch the vulnerability but not technically feasible to do so as required by Paragraph 1.1(a)(i), then as soon as reasonably practicable after the public release;

17.1.2 the Supplier must patch any vulnerabilities classified as "important":

(i) if it is technically feasible to do so, within 1 month of the public release; or

(ii) if it is technical feasible to patch the vulnerability but not technically feasible to do so as required by Paragraph 1.1(a)(i), then as soon as reasonably practicable after the public release;

17.1.3 the Supplier must remedy any vulnerabilities classified as "other" in the public release:

(i) if it is technically feasible to do so, within 2 months of the public release; or

(ii) if it is technical feasible to remedy the vulnerability but not technically feasible to do so as required by Paragraph 1.1(a)(i), then as soon as reasonably practicable after the public release; or

17.1.4 where it is not technically feasible to patch the vulnerability, the Supplier must implement appropriate technical and organisational measures to mitigate the risk posed by the vulnerability.

18. Malware protection

18.1 The Supplier shall install and maintain Anti-virus Software or procure that Anti-virus Software is installed and maintained on the Supplier System.

18.2 The Supplier must ensure that such Anti-virus Software:

18.2.1 prevents the installation of the most common forms of Malicious Software in the Supplier System;

18.2.2 performs regular scans of the Supplier System to check for Malicious Software; and

18.2.3 where Malicious Software has been introduced into the Supplier System, so far as practicable:

(i) prevents the harmful effects from the Malicious Software; and

(ii) removes the Malicious Software from the Supplier System.

19. End-user Devices

19.1 The Supplier must, and must ensure that all Subcontractors, manage all End-user Devices on which Buyer Data is stored or Handled in accordance with the following requirements:

19.1.1 the operating system and any applications that store, Handle or have access to Buyer Data must be in current support by the vendor, or the relevant community in the case of open source operating systems or applications;

19.1.2 users must authenticate before gaining access;

19.1.3 all Buyer Data must be encrypted using a suitable encryption tool;

19.1.4 the End-user Device must lock and require any user to re-authenticate after a period of time that is proportionate to the risk environment, during which the End-user Device is inactive;

19.1.5 the End-User Device must be managed in a way that allows for the application of technical policies and controls over applications that have access to Buyer Data to ensure the security of that Buyer Data;

19.1.6 the Supplier or Subcontractor, as applicable, can, without physical access to the End-user Device, remove or make inaccessible all Buyer Data stored on the device and prevent any user or group of users from accessing the device; and

19.1.7 all End-user Devices are within the scope of any required Certification.

19.2 The Supplier must comply, and ensure that all Subcontractors comply, with the recommendations in NCSC Device Guidance as if those recommendations were incorporated as specific obligations under this Contract.

20. **Vulnerability scanning**

20.1 The Supplier must:

20.1.1 scan the Supplier System at least once every month to identify any unpatched vulnerabilities; and

20.1.2 if the scan identifies any unpatched vulnerabilities, ensure they are patched in accordance with Paragraph 17.

21. **Access control**

21.1 The Supplier must, and must ensure that all Subcontractors:

21.1.1 identify and authenticate all persons who access the Supplier System before they do so;

21.1.2 require multi-factor authentication for all user accounts that have access to Buyer Data or that are Privileged Users;

21.1.3 allow access only to those parts of the Supplier System and Sites that those persons require; and

21.1.4 maintain records detailing each person’s access to the Supplier System.

21.2 The Supplier must ensure, and must ensure that all Subcontractors ensure, that the user accounts for Privileged Users of the Supplier System:

21.2.1 are allocated to a single, individual user;

21.2.2 are accessible only from dedicated End-user Devices;

21.2.3 are configured so that those accounts can only be used for system administration tasks;

21.2.4 require passwords with high complexity that are changed regularly;

21.2.5 automatically log the user out of the Supplier System after a period of time that is proportionate to the risk environment during which the account is inactive; and

21.2.6 are:

(i) restricted to a single role or small number of roles;

(ii) time limited; and

(iii) restrict the Privileged User's access to the internet.

22. **Remote Working**

22.1 The Supplier must ensure, and ensure that Sub-contractors ensure, that:

22.1.1 unless in writing by the Buyer, Privileged Users do not undertake Remote Working; and

22.1.2 where the Buyer permits Remote Working by Privileged Users, the Supplier ensures, and ensures that Sub-contractors ensure, that such Remote Working takes place only in accordance with any conditions imposed by the Buyer.

22.2 Where the Supplier or a Sub-contractor wishes to permit Supplier Staff to undertake Remote Working, it must:

22.2.1 prepare and have approved by the Buyer the Remote Working Policy in accordance with this Paragraph;

22.2.2 undertake and, where applicable, ensure that any relevant Sub-contractors undertake, all steps required by the Remote Working Policy;

22.2.3 ensure that Supplier Staff undertake Remote Working only in accordance with the Remote Working Policy; and

22.2.4 may not permit any Supplier Staff of the Supplier or any Sub-contractor to undertake Remote Working until the Remote Working Policy is approved by the Buyer.

22.3 The Remote Working Policy must include or make provision for the following matters:

22.3.1 restricting or prohibiting Supplier Staff from printing documents in any Remote Location;

22.3.2 restricting or prohibiting Supplier Staff from downloading any Buyer Data to any End-user Device other than an End User Device that:

(i) is provided by the Supplier or Sub-contractor (as appropriate); and

(ii) complies with the requirements set out in Paragraph 3 (*End-user Devices*);

22.3.3 ensuring that Supplier Staff comply with the Expected Behaviours (so far as they are applicable);

22.3.4 giving effect to the Security Controls (so far as they are applicable); and

22.3.5 for each different category of Supplier Staff subject to the proposed Remote Working Policy:

(i) the types and volumes of Buyer Data that the Supplier Staff can Handle in a Remote Location and the Handling that those Supplier Staff will undertake;

(ii) any identified security risks arising from the proposed Handling in a Remote Location;

(iii) the mitigations, controls and security measures the Supplier or Sub-contractor (as applicable) will implement to mitigate the identified risks; and

(iv) the business rules with which the Supplier Staff must comply.

22.4 The Supplier may submit a proposed Remote Working Policy to the Buyer for consideration at any time.

23. **Backup and recovery of Buyer Data**

23.1 The Supplier must ensure that the Supplier System:

23.1.1 backs up and allows for the recovery of Buyer Data to achieve the recovery point and recovery time objectives specified by the Buyer, or in accordance with Good Industry Practice where the Buyer has not specified; and

23.1.2 retains backups of the Buyer Data for the period specified by the Buyer, or in accordance with Good Industry Practice where the Buyer has not specified.

23.2 The Supplier must ensure the Supplier System:

23.2.1 uses backup location for Buyer Data that are physically and logically separate from the rest of the Supplier System;

23.2.2 the backup system monitors backups of Buyer Data to:

(i) identifies any backup failure; and

(ii) confirm the integrity of the Buyer Data backed up;

23.2.3 any backup failure is remedied promptly;

23.2.4 the backup system monitors the recovery of Buyer Data to:

(i) identify any recovery failure; and

(ii) confirm the integrity of Buyer Data recovered; and

23.2.5 any recovery failure is promptly remedied.

23.3 The Supplier must ensure that the Supplier System backups is immutable.

24. **Return and deletion of Buyer Data**

24.1 Subject to Paragraph 24.2, when requested to do so by the Buyer, the Supplier must, and must ensure that all Subcontractors:

24.1.1 securely erase any or all Buyer Data held by the Supplier or Subcontractor using a deletion method that ensures that even a determined expert using specialist techniques can recover only a small fraction of the data deleted; or

24.1.2 provide the Buyer with copies of any or all Buyer Data held by the Supplier or Subcontractor using the method specified by the Buyer.

24.2 Paragraph 24.1 does not apply to Buyer Data:

24.2.1 that is Personal Data in respect of which the Supplier is a Controller;

24.2.2 to which the Supplier has rights to Handle independently from this Contract; or

24.2.3 in respect of which, the Supplier is under an obligation imposed by Law to retain.

24.3 The Supplier must, and must ensure that all Sub-contractors, provide the Buyer with copies of any or all Buyer Data held by the Supplier or Sub-contractor:

24.3.1 when requested to do so by the Buyer; and

24.3.2 using the method specified by the Buyer.

25. **Physical security**

25.1 The Supplier must, and must ensure that Subcontractors, store the Buyer Data on servers housed in physically secure locations.

26. **Breach of Security**

26.1 If the Supplier becomes aware of a Breach of Security that impacts or has the potential to impact the Buyer Data, it shall:

26.1.1 notify the Buyer as soon as reasonably practicable after becoming aware of the breach, and in any event within 24 hours;

26.1.2 provide such assistance to the Buyer as the Buyer requires until the Breach of Security and any impacts or potential impacts on the Buyer are resolved to the Buyer's satisfaction;

26.1.3 where the Law requires the Buyer to report a Breach of Security to the appropriate regulator provide such information and other input as the Buyer requires within the timescales specified by the Buyer; and

26.1.4 where the Breach of Security results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data, undertake any communication or engagement activities required by the Buyer with the individuals affected by the Breach of Security.